IN THE CLAIMS

1. – 30. (Canceled)

31. (Currently Amended) A system for enabling an outside entity to control devices at a location, the system comprising:

(a) an internal computer system associated with the location;

(b) a sensing apparatus associated with the internal computer system, wherein the sensing apparatus can detect a triggering event at the location;

(c) a firewall in communication with the internal computer system, wherein the firewall is adapted to verify identity information associated with the outside entity; and

(d) a device associated with the internal computer system, wherein the device can be controlled by the outside entity via the internal computer system,

wherein when the sensing apparatus detects the triggering event the internal computer system establishes a communication session with the outside entity via an public ~~external computer~~communications network in direct communication with the location, the public communications network including at least one of a public switched telephone network and a wireless communication link,

wherein the outside entity provides identity information to the internal computer system,

wherein the firewall creates a secured tunnel for the outside entity to access the internal computer system,

wherein the outside entity uses information retrieved from a database to control the device during the communication session, and

wherein only the outside entity can terminate the communication session.

32. (Original) The system of claim 31, wherein the identity information comprises a password.

33. (Original) The system of claim 31, wherein the identity information comprises a digital certificate.

34. (Original) The system of claim 33, wherein the digital certificate is authenticated by a certificate authority.

35. (Canceled)

36. (Currently Amended) A method for enabling an outside entity to control devices at a location, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location;

(b) reporting a triggering event associated with the location to the outside entity via a public communications network in direct communication with the location, the public communications network including at least one of a public switched telephone network and a wireless communication link;

(c) initiating a communication session between the internal computer system and the outside entity through a secure tunnel over an external computer network, wherein the communication session is initiated by the internal computer network;

(d) verifying identity information provided by the outside entity; and

(e) allowing the outside entity to control the device during the communication session,

wherein only the outside entity can terminate the communication session.

37. (Original) The method of claim 36, wherein the identity information is a password issued to the outside entity by the internal computer system.

38. (Original) The method of claim 36, wherein the identity information is a digital certificate issued to the outside entity by a certificate authority.

39. (Original) The method of claim 38, wherein the step of verifying the identity information of the outside entity is performed by the certificate authority.

40. (Original) The method of claim 36, further comprising the step of authenticating identity of the internal computer system for the outside entity.

41. (Currently Amended) A method for enabling an outside entity to handle a situation at a location, the method comprising the steps of:

(a) associating at least one device with an internal computer system at the location;

(b) reporting a triggering event associated with the situation at the location to the outside entity via a public communications network in direct communication with the location, the public communications network including at least one of a public switched telephone network and a wireless communication link;

(c) initiating a communication session between the internal computer system and the outside entity through an external computer network;

(d) providing a first identity information associated with the internal computer system to the outside entity;

(e) providing a second identity information associated with the outside entity to the internal computer system;

(f) authenticating both the first identity information and the second identity information;

(g) establishing a secured tunnel through a firewall associated with the internal computer system if both the first identity information and the second identity information are authenticated; and

(h) allowing the outside entity to control the device to handle the situation during the communication session,

wherein only the outside entity can terminate the communication session.

42. (Original) The method of claim 41, wherein the first identity information is a first digital certificate issued to the internal computer system by a certificate authority.

43. (Canceled)

44. (Original) The method of claim 41, wherein the step of authenticating both the first identity information and the second identity information is performed by a certificate authority.

45. (Previously Presented) The method of claim 41, wherein the triggering event is a call from a voice-over-Internet-protocol (VOIP) device.

46. (Canceled)